THE PRIVATE LIFE OF DRM: LESSONS ON INFORMATION PRIVACY FROM THE COPYRIGHT ENFORCEMENT DEBATES

Rebecca Wexler [1]

17 YALE J.L. & TECH. 368 (2015)

ABSTRACT

This Article presents an intellectual history of competing privacy claims and counterclaims in policy debates about copyright enforcement methods. Specifically, it examines debates over Digital Rights Management technologies, or encryption tools that track the use of, and restrict access to, copyrighted information. The Article finds that, historically, information privacy claims in these debates did not lead to determinant outcomes; each argument drawn from a privacy interest corresponds to a counterclaim drawn from that same interest but supporting an opposite policy preference. Moreover, these competing claims on privacy cannot be explained as mere superficial semantics. Rather, they concern a variety of substantive concepts of information privacy interests. This observation suggests that claims on information privacy are unstable, and may unintentionally bolster the positions that their proponents intend to reject. The Article cautions against adopting new definitions of privacy interests for the digital age, and in favor of focusing policy choices on who uses new technologies and for what ends.

[1] Rebecca Wexler is a member of the Yale Law School J.D. Class of 2016 and a Fellow of the Information Society Project. This Article received the 2014 Nathan Burkan Prize for Best Paper in the Field of Copyright Law at Yale Law School. The author is grateful to BJ Ard, Jack Balkin, Gautam Bhatia, Kiel Brennan-Marquez, Amy Kapczynski, Ben Picozzi, and Megan Wright for their generous feedback on earlier drafts. Eric Fish and Samantha Godwin offered helpful suggestions. The author thanks Adam Adler, Amanda Lynch, Brianna van Kan, Jimmy Zhuang and the editors of the *Yale Journal of Law and Technology* for their excellent editorial work.

TABLE OF CONTENTS

Introduction

In the spring and summer of 2012, the German branch of the European Pirate Party—a group of privacy advocates—campaigned for and won seats in four state parliaments across Germany. Their platform called for reforming copyright enforcement practices, arguing that certain encryption tools to track and restrict individuals' use of copyrighted information, known as Digital Rights Management (DRM) technologies, threaten privacy. Information privacy claims thus became a means for Pirates to oppose both the use of these tools and statutes that prohibit disabling them, known as anti-circumvention laws. This strategy was not new. Arguments about the privacy costs of DRM-enabled copyright enforcement are well represented in legal scholarship.

This Article argues that information privacy claims, both in DRM debates and perhaps more broadly, risk buttressing the very policies they are meant to reform. It traces the intellectual history of DRM-related privacy arguments using the following sources: Pirate political platforms; privacy law scholarship; and the legislative and diplomatic histories of three anti-circumvention laws—the Digital Millennium Copyright Act (DMCA); the World Intellectual Property Organization (WIPO)

Copyright Treaty; and the WIPO Performances and Phonograms Treaty. Comparing and contrasting these historical debates shows that advocates both for and against DRM invoked similar privacy interests to justify opposing policies. Appeals on both sides self-identified as pro-privacy but made opposite forecasts about the effects of DRM and anti-circumvention laws on privacy itself. In other words, the debates illustrate what Albert Hirschman termed the "perversity thesis," whereby reactionaries—whether conservative or progressive—claim that a proposed action "will produce, via a chain of unintended consequences, the *exact contrary* of the objective being claimed and pursued."[2]

Competing privacy claims about DRM cannot be explained as mere superficial semantics. Rather, I contend, they reflect deeper theories of information privacy in current legal scholarship debates. Part I presents a brief overview of past and present scholarly efforts to conceptualize information privacy, including property-based, spatial, contextual, anonymity-based, substantive, and material understandings of privacy interests. The Article then shows how each of these understandings led to indeterminate results in practice. Basic context is provided in Part II, which details various types of DRM technologies, outlines their expanding use in a world of ever-increasing connectivity, and surveys some of the advocacy campaigns to reform them. In Part III, I consider how different theories of information privacy functioned in this context. I find that arguments drawn from the various conceptions of privacy interests explored in Part I each corresponded to plausible counterclaims drawn from those same privacy interests.

Part IV presents and critiques four plausible explanations for these observations. It concludes that who makes privacy claims may better predict their outcomes than the theoretical understandings from which they are derived. Further refining abstract definitions of information privacy is thus unlikely to increase its determinacy. For those seeking to protect privacy in the digital age, whose privacy, not what privacy, should be of primary concern.

I. Conceptual Instability: Information, Substantive, and Intellectual Privacy

Conceptual instability may render privacy claims particularly vulnerable to "perverse" redeployment. While privacy has long been an elusive concept, recent technological changes have intensified its ambiguities. Today, courts and commentators alike are struggling to define privacy—and

---

[2] ALBERT O. HIRSCHMAN, THE RHETORIC OF REACTION: PERVERSITY, FUTILITY, JEOPARDY 11 (1991).

especially privacy interests in personally identifiable information—for the digital age.[3] The DRM debates are a particularly interesting example.

Scholarly debate over privacy's ideal attributes and legal protections has proliferated over the past decades as technological capacity to render them ineffective has expanded. Some strands of contemporary privacy law scholarship seek to identify categories of information that warrant enhanced privacy protections.[4] Others conceptualize privacy as a form of property and proffer transactional models to let markets determine the safeguards for personal information,[5] or deem privacy as a form of collective resource to be "cultivated."[6] Still others argue that information privacy is fluid and that its protections should track independent variables such as social context,[7] the relationship between parties to a communication,[8]

---

[3] *See, e.g.*, United States v. Jones, 132 S. Ct. 945, 962 (2012) (Alito, J., concurring) ("The *Katz* expectation-of-privacy test [assumes] a well-developed and stable set of privacy expectations. But technology can change those expectations."); *cf.* Julie E. Cohen, *Examined Lives: Informational Privacy and the Subject as Object*, 52 STAN. L. REV. 1373, 1436 (2000) ("It has become commonplace . . . to assert that legal guarantees of privacy will be rendered empty by rapid technological change.").

[4] *See, e.g.*, BJ Ard, *Confidentiality and the Problem of Third Parties: Protecting Reader Privacy in the Age of Intermediaries*, 16 YALE J. L. & TECH. 1, 4 (2013) (arguing that confidentiality obligations should be defined "with reference to the content we wish to protect rather than the actors we suppose will possess it"); Julie E. Cohen, *A Right to Read Anonymously: A Closer Look at "Copyright Management" in Cyberspace*, 28 CONN. L. REV. 981, 982 (1996) (advocating heightened privacy protections for information about reading practices); Neil M. Richards, *The Perils of Social Reading*, 101 GEO. L.J. 689, 691 (2013) (arguing that "records of our reading and movie watching deserve special protection compared to other kinds of personal information").

[5] *See, e.g.*, Lauren Henry, *Privacy as Quasi-Property*, 100 IOWA L. REV. __ (forthcoming 2015) (manuscript at 12), *available at* http://papers.ssrn.com/sol3/papers.cfm?abstract_id=2567579 [http://perma.cc/DB3D-BJ4K] ("I argue that conceptualizing privacy as quasi-property is a superior approach with many analytical advantages over both privacy as property and privacy as a personal interest."); Pamela Samuelson, *Privacy as Intellectual Property?*, 52 STAN. L. REV. 1125, 1172 (2000) ("One of the virtues of a contractual approach to protecting information privacy is that it can accommodate the multiple interests people have in personal information . . . .").

[6] Bryan H. Choi, *A Prospect Theory of Privacy*, 51 IDAHO L. REV. 623, 626 (2015).

[7] *See, e.g.*, Helen Nissenbaum, *Privacy as Contextual Integrity*, 79 WASH. L. REV. 119, 137-38, 155 (2004) (arguing that societal norms govern the flow of personal information in different contexts, and that privacy interests attach to maintain the "contextual integrity" of that information as it travels between social spheres).

[8] *See, e.g.*, Kiel Brennan-Marquez, *Fourth Amendment Fiduciaries*, 84 FORDHAM L. REV. __ (forthcoming 2015) (manuscript at 4) (on file with author) ("The implication of A's decision to share information with B should [depend] on the role B plays in the world vis-à-vis A."); Jack

or how transparent the end uses of information are to those who generate it.[9]

The present conversation reflects deep historic roots; privacy has long eluded stable legal definition. To start, it boasts chimeric roots in common law, statutes, and the "penumbras" of the Bill of Rights.[10] In their foundational 1890 article, Samuel Warren and Louis Brandeis described privacy as the right "to be let alone."[11] Seventy years later, William Prosser articulated four privacy torts: intrusion upon seclusion; the public disclosure of private facts; publicity in false light; and the appropriation of name or likeness.[12]

Recent commentators have described an even more diverse array of privacy interests. Daniel Solove, for instance, characterizes privacy as an umbrella concept encompassing a series of distinct harms that share mere family resemblance. These harms include dignitary injuries, power imbalances, and the chilling effects caused by the risk of future injury.[13] Activities that can produce such harms include the collection, processing, and dissemination of information by both private parties and the government,[14] intrusions into protected spaces like the home, and government interference with certain privileged personal decisions such as reproductive and sexual choices. Solove terms the latter "decisional interferences."[15]

Others draw fewer categories. The Court in *Whalen v. Roe*, for example, identified two separate elements in privacy case law: "One is the individual interest in avoiding disclosure of personal matters, and another is the interest in independence in making certain kinds of important decisions."[16] Commenting

---

Balkin, *Information Fiduciaries in the Digital Age*, BALKINIZATION (Mar. 5, 2014, 4:50 PM), http://balkin.blogspot.com/2014/03/information-fiduciaries-in-digital-age.html [http://perma.cc/86YH-YY7N] ("The concept of an information fiduciary helps us understand how we might protect digital privacy while not running afoul of the First Amendment.").

9 *See, e.g.*, Wendy Seltzer, Privacy, Option Value, and Feedback 24 (Aug. 15, 2012) (unpublished manuscript), http://papers.ssrn.com/sol3/papers.cfm?abstract_id=2032100 [http://perma.cc/P6A2-9FUR] ("The notion of privacy-feedback can bridge the gap between contextual privacy and the privacy-as-secrecy paradigm.").

10 Griswold v. Connecticut, 381 U.S. 479, 484 (1965).

11 Samuel D. Warren & Louis D. Brandeis, *The Right to Privacy*, 5 HARV. L. REV. 193, 205 (1890). *See also*, Josh Blackman, Brian L. Frye, & Michael McCloskey, *Justice John Marshall Harlan: Professor of Law*, 81 GEO. WASH. L. REV. 1063, 1113 (2013) (noting that the Warren and Brandeis theory of privacy contrasted with Justice Harlan's contemporary view of press freedoms).

12 William L. Prosser, *Privacy*, 48 CAL. L. REV. 383, 389 (1960).

13 Daniel J. Solove, *A Taxonomy of Privacy*, 154 U. PA. L REV. 477, 487-88 (2006).

14 *Id.* at 489.

15 *Id.* at 557-59.

16 Whalen v. Roe, 429 U.S. 589, 599-60 (1977).

on this decision, Sonia Katyal has termed the first an "informational privacy" interest, and the second a "substantive privacy interest." She points out that the Supreme Court offers less protection to the first, which is governed primarily by statutory and regulatory authorities, than to the second, which is constitutionally protected.[17]

Yet, even these two categories—informational and substantive—can blend together in certain types of privacy claims. Neil Richards has coined the term "intellectual privacy" to describe the ability "to develop ideas and beliefs away from the unwanted gaze or interference of others."[18] "Intellectual privacy" concerns the records of activities that can act as proxies for thoughts about politics, religion, sex, or similar issues (for example, one's Internet search history, library records, or anonymous political donations).[19] This concept thus recognizes that the collection, processing, and dissemination of information can in and of itself interfere with cognitive—and hence on some level decisional—autonomy.[20] In other words, information privacy can incorporate personal autonomy, or substantive, elements.

As the following Parts will show, advocates in the DRM debates have launched privacy claims that track many of these theories and more, mobilizing different conceptions of privacy for varied goals.

II. Digital Rights Management

A. *The Tools*

Digital Rights Management (DRM) is a type of technological self-help for copyright enforcement similar to a digital lock.[21] DRM technologies can control access to

---

[17] Sonia Katyal, *The New Surveillance*, 54 CASE W. RES. L. REV. 297, 308-09 (2003) ("Today, informational privacy derives its force from a panoply of federal, state, and regulatory guidelines . . . .").

[18] Neil M. Richards, *Intellectual Privacy*, 87 TEX. L. REV. 387, 389 (2008).

[19] *Id.*

[20] *See, e.g.*, Julie E. Cohen, *DRM and Privacy*, 18 BERKELEY TECH. L.J. 575, 582 (2003) ("[A] strand of privacy theory . . . emphasizes decisional autonomy as the basis for at least some privacy rights. Some philosophers argue that where certain deeply personal activities are concerned, privacy denotes not only a condition of (relative) inaccessibility, but also a zone of noninterference with individual choice.").

[21] Other terms that apply to these technologies include Technological Protection Measures (TPM); Electronic Copyright Management Systems (ECMS); Content Protection Software; "trusted systems"; Rights Management Systems; Enterprise Rights Management (ERM); and Rights Management Information (RMI).

information and authenticate, encrypt, and track content to monitor its use.[22]

DRM access controls restrict how digital content can be used, how long it is available, or the number of times that users can play, stream, download, or copy it. For instance, DRM may limit interoperability to prevent users from accessing content on different devices or in different geographic regions.[23] It can also tie digital content to a single user account and a particular online delivery ecosystem to prevent users from sharing products with others.[24] Further, access controls empower rights holders to punish individual users for alleged violations of copyright law or contract by terminating their access entirely. To illustrate, in 2009 Amazon remotely wiped all kindle copies of the books *Animal Farm* and *1984* that well-meaning customers had obtained from one bad acting content provider who was violating the copyright.[25] During the process, Amazon also deleted customers' notes and highlights, exacerbating the invasion into users' personal papers.[26]

DRM that tracks user behavior can collect information such as where, when, what, and how much of a media file an individual consumes. Some DRM embeds triggers into digital files to monitor use post-sale.[27] Others generate unique identifying patterns to brand and trace files.[28] Automated search technologies then scour websites for files containing these patterns and alert rights holders to their location.[29] An example on the market in 2013, called SiDiM, varies the text of each copy of an e-book slightly so that it can be traced if shared

---

[22] *See, e.g.*, LAWRENCE HARTE, INTRODUCTION TO DIGITAL RIGHTS MANAGEMENT (DRM); IDENTIFYING, TRACKING, AUTHORIZING AND RESTRICTING ACCESS TO DIGITAL MEDIA 1 (2006).

[23] *Protecting and Empowering Consumers in the Purchase of Digital Content Products* 5, 26 (OECD Digital Economy Papers no. 219, 2013), http://dx.doi.org/10.1787/5k49czlc7wd3-en [http://perma.cc/7R7B-YCMA] [hereinafter *Digital Content Products*].

[24] Roberto Baldwin, *New DRM Will Change the Words in Your E-Book*, WIRED, June 17, 2013, http://www.wired.com/2013/06/new-ebook-drm [http://perma.cc/S7XE-SNRY] ("stripping the DRM from any of the e-books purchased at the big-name stores is as easy as downloading an app").

[25] Brad Stone, *Amazon Erases Orwell Books from Kindle*, N.Y. TIMES (Jul. 17, 2009) http://www.nytimes.com/2009/07/18/technology/companies/18amazon.html [http://perma.cc/AM3Z-HC4Y].

[26] Teenager Justin Gawronski sued after losing his notes for a school project. *E.g.*, Jonathan Potter, *The E-Book and the Surveillance Society*, SECOND NATURE (Nov. 13, 2013), http://secondnaturejournal.com/the-e-book-and-the-surveillance-society [http://perma.cc/VH75-6TFB].

[27] HARTE, *supra* note 22, at 63.

[28] This type of technological protection measure is sometimes referred to as Rights Management Information. *See, e.g.*, World Intellectual Property Organization Copyright Treaty art. 12, Dec. 20, 1996, 36 I.L.M. 65 [hereinafter WCT].

[29] HARTE, *supra* note 22, at 62.

online—even if shared legally.[30] DRM may also protect underlying devices that track user information. Samsung "smart televisions," for instance, have built-in DRM support[31] are now capable of monitoring and recording voice conversations inside a home.[32]

Today, DRM usage is on the rise. The growth of mobile devices—as opposed to general-purpose personal computers—has meant that DRM-controlled infrastructure now pervades our communications ecology. Apple adds DRM to every application available for the Apple Watch, iPhone, iPod, and iPad.[33] The latest version of HTML5, the Web's core computer language, supports the delivery of DRM-protected content directly within browsers without resort to supplemental plug-ins such as Flash.[34] Because the DRM module is closed-source, HTML5 browsers can no longer provide fully open-source access to the Web and users now interact with more content through DRM by default.[35]

Perhaps most transformative, manufacturers have begun to incorporate DRM into the tangible physical objects that constitute our built environments, such as cars, household

---

[30] *See, e.g.*, Baldwin, *supra* note 24.

[31] *Platforms*, DRMTODAY, http://www.drmtoday.com/platforms [http://perma.cc/Y9UE-DZKZ] (last visited Apr. 15, 2015) (describing the types of DRM on a variety of devices).

[32] Complaint, Request for Investigation, Injunction, and Other Relief at 1, 4, *In the Matter of Samsung Electronics Co., Ltd.* (F.T.C. Feb. 24, 2015), https://epic.org/privacy/internet/ftc/Samsung/EPIC-FTC-Samsung.pdf [https://perma.cc/5XNT-ECF5].

[33] *See, e.g.*, Reuven Ashtar, *Licensing as Digital Rights Management, from the Advent of the Web to the iPad*, 13 YALE J. L. & TECH. 141, 153, 186 (2011) (describing the iPad and iPhone DRM systems); Chris Foresman, *Apple Fixes App Store DRM Error, Crash-Free Downloads Resume*, ARSTECHNICA (July 6, 2012, 3:53 PM), http://arstechnica.com/apple/2012/07/apple-fixes-app-store-drm-error-crash-free-downloads-resume [http://perma.cc/9MJL-GBD8]; *Apple is Defective by Design*, DEFECTIVE BY DESIGN, https://defectivebydesign.org/apple [https://perma.cc/TR74-7H2T] (last visited June 1, 2015) ("Apple corporate headquarters keeps a tight lock on the apps available for its mobile operating system (iOS) . . . .").

[34] *See, e.g.*, *Encrypted Media Extensions*, GITHUB, https://w3c.github.io/encrypted-media (last visited Aug. 11, 2015) ("Implementation of Digital Rights Management is not required for compliance with this specification."); Danny O'Brien, *International Day Against DRM: Whatever Happened to the W3C?*, EFF DEEPLINKS BLOG (May 6, 2014), https://www.eff.org/deeplinks/2014/05/international-day-against-drm-whatever-happened-w3c [https://perma.cc/X3A5-PC3L].

[35] Mozilla explained this consequence well when it announced attempts to mitigate privacy risks by wrapping DRM content delivery in an open-source sandbox, increasing transparency about what information gets collected. Andreas Gal, *Reconciling Mozilla's Mission and W3C EME*, HACKS.MOZILLA.ORG (May 14, 2014), https://hacks.mozilla.org/2014/05/reconciling-mozillas-mission-and-w3c-eme/ [https://perma.cc/ZY3B-SQR2].

items, and even medical devices. In short, DRM has leapt into the array of "smart" objects sometimes referred to as the Internet of Things, including light bulbs,[36] litter boxes,[37] cars,[38] and even coffee makers.[39] This development threatens to increase invasions of information privacy and to promote new intrusions into locational privacy and bodily autonomy.[40] As journalist Cory Doctorow put it more poetically, "when I get into a car—a computer that I put my body into—with my hearing aid—a computer I put inside my body—I want to know that these technologies are not designed to keep secrets from me, or to prevent me from terminating processes on them that work against my interests."[41] This broad new array of computational devices means that DRM increasingly controls "processes" that collect sensitive information not merely about media consumption but also about location, intimate bodily functions, and more.

B. *The Laws*

---

[36] *See, e.g.*, Tim Cushing, *DRM; Or How to Make 30,000-Hour LED Bulbs 'Last' Only One Month*, TECHDIRT (Mar. 18, 2015 6:14AM), https://www.techdirt.com/articles/20150317/08091030343/drm-how-to-make-30000-hour-led-bulbs.shtml [https://perma.cc/VNE5-FZNA].

[37] *See, e.g.*, Tim Cushing, *DRM; Or How to Turn Your Cat's Litter Box Into an Inkjet Printer*, TECHDIRT (Jan. 8, 2015 6:08 AM), https://www.techdirt.com/articles/20150102/09574429580/drm-how-to-turn-your-cats-litter-box-into-inkjet-printer.shtml [https://perma.cc/AG7D-ZMBE].

[38] *See, e.g.*, Petition of Electronic Frontier Foundation, In the Matter of Exemption to Prohibition on Circumvention of Copyright Protection Systems for Access Control Technologies (No. 2014-07), https://www.eff.org/document/eff-autos-repair-and-modification-exemption-request [https://perma.cc/HM3Z-DE52]. *See also* Parker Higgins, *DRM in Cars Will Drive Consumers Crazy*, EFF DEEPLINKS BLOG (Nov. 13, 2013), https://www.eff.org/deeplinks/2013/11/drm-cars-will-drive-consumers-crazy [https://perma.cc/G864-DY2B]; Kyle Wiens, *WTF! It Should Not Be Illegal to Hack Your Own Car's Computer*, WIRED (Jan. 23, 2015 6:00 AM), http://www.wired.com/2015/01/let-us-hack-our-cars [https://perma.cc/TZ2G-4D6E].

[39] *See, e.g.*, Karl Bode, *Keurig Will Use DRM in New Coffee Maker to Lock Out Refill Market*, TECHDIRT (Mar. 3, 2014 5:32 AM), https://www.techdirt.com/articles/20140227/06521826371/keurig-will-use-drm-new-coffee-maker-to-lock-out-refill-market.shtml [https://perma.cc/6VTJ-RTU8].

[40] *See, e.g.*, Edith Ramirez, Chairwoman, Fed. Trade Comm'n, Privacy and the IoT: Navigating Policy Issues, Opening Remarks at the International Consumer Electronics Show (Jan 6. 2015) ("The introduction of sensors and devices into currently intimate spaces—like our homes, cars, and even our bodies—poses particular challenges and increases the sensitivity of the data that is being collected.").

[41] Cory Doctorow, *Lockdown: The Coming War on General-Purpose Computing*, BOINGBOING (Jan. 10, 2012), http://boingboing.net/2012/01/10/lockdown.html [http://perma.cc/X78F-JZDK].

The term DRM can refer to a diverse set of tools that often go by other names.[42] This Article uses it as a catchall to describe any application of a technology that would qualify for legal protection under U.S. or international law.

Both U.S. law and international treaties protect DRM from circumvention, or efforts to disable the technology and thereby to evade its intended copyright enforcement capacities.[43] Section 1201 of the U.S. Digital Millennium Copyright Act (DMCA) prohibits circumventing "a technological measure that effectively controls access to a work protected [by copyright]."[44] The World Intellectual Property Organization (WIPO) is a United Nations agency representing 188 member states. WIPO focuses on intellectual property issues and has enacted two particularly relevant international treaties: the WIPO Copyright Treaty and the WIPO Performances and Phonograms Treaty.[45] Both treaties require member states to "provide adequate legal protection and effective legal remedies against the circumvention of effective technological measures that are used by [rights holders] in connection with the exercise of their [copyrights]."[46] Similarly, leaked copies of the Trans-Pacific Partnership Agreement show the Agreement prohibiting circumventing "any effective technological measure that controls access to a protected work . . . ."[47]

C. *The Advocacy Campaigns*

Pro-privacy efforts to reform DRM usage and anti-circumvention laws have emerged in response to the proliferation of DRM technologies. On January 20, 2015,

---

[42] *See, e.g.*, Ashtar, *supra* note 33 (describing DRM as an "umbrella term," criticizing courts for "indiscriminately protecting DRM measures," and arguing that "not all digital locks and contractual notices qualify for [DMCA anti-circumvention] legal protection").

[43] For an excellent overview of the legal protections of DRM that prohibit its circumvention, see Urs Gasser, *Legal Frameworks and Technological Protection of Digital Content: Moving Forward Towards a Best Practice Model*, 17 FORDHAM INTELL. PROP. MEDIA & ENT. L.J. 39, 43-65 (2006).

[44] Digital Millennium Copyright Act of 1998, 17 U.S.C. § 1201 (2012).

[45] *Inside WIPO*, WORLD INTELLECTUAL PROP. ORG., http://www.wipo.int/about-wipo/en/index.html [http://perma.cc/T9DF-CL42] (last visited Aug. 8, 2015). For helpful context on WIPO's role in intellectual property law enforcement, see Margot E. Kaminski, *The Capture of International Intellectual Property Law Through the U.S. Trade Regime*, 87 S. CAL. L. REV. 977, 984 (2014).

[46] WCT, *supra* note 28, art. 11; World Intellectual Property Organization Performances and Phonograms Treaty art. 18., Dec. 20, 1996, 36 I.L.M. 76 [hereinafter WPPT].

[47] TPP Treaty: Intellectual Property [Rights] Chapter, Consolidated Text, Oct. 5, 2015, Art. QQ.G.10 at 33 (Wikileaks released on Oct. 9, 2015), https://wikileaks.org/tpp-ip3/WikiLeaks-TPP-IP-Chapter/WikiLeaks-TPP-IP-Chapter-051015.pdf [https://perma.cc/2AZC-KTMZ] [hereinafter TPP IP Chapter].

Doctorow and the Electronic Frontier Foundation (EFF), a digital rights advocacy organization, launched the Apollo 1201 Project "mission to eradicate DRM in our lifetime."[48] They seek to repeal anti-circumvention laws and to encourage industry to adopt alternative copyright enforcement strategies.[49] Apollo 1201 joins the likeminded "Defective by Design" campaign, launched almost a decade ago by the Free Software Foundation, to "eliminate DRM as a threat to . . . privacy . . . ."[50] Some international laws have begun to reflect these concerns. Article 27 of the 2011 Anti-Counterfeiting Trade Agreement multinational treaty, for instance, obliges contracting parties to adopt "adequate" legal protections and remedies against circumvention.[51] But it also calls on member states to adopt enforcement procedures that preserve "privacy," and to encourage businesses to do the same.[52]

One campaign that has achieved widespread visibility in recent years is that of the European Pirate Party. Pirates are a social and political movement that coalesced around issues of copyright reform and information privacy.[53] The movement began in 2006 when a group of Swedish computer programmers founded the first Pirate Party.[54] Widespread protests over a police crackdown on the file-sharing search engine The Pirate Bay (TPB) propelled the group into what communications scholar Patrick Burkart has called a movement for "communicative freedom."[55] Pirates gained their first seat in the European parliamentary election of 2009.[56] Two years later, they won fifteen seats in the Berlin State Parliament,[57]

---

48 Press Release, Elec. Frontier Found., Cory Doctorow Rejoins EFF to Eradicate DRM Everywhere (Jan. 20, 2015), https://www.eff.org/press/releases/cory-doctorow-rejoins-eff-eradicate-drm-everywhere [https://perma.cc/DR6Y-5W56].

49 *Id.*

50 *About Defective by Design*, DEFECTIVE BY DESIGN, http://www.defectivebydesign.org/about_defectivebydesign [http://perma.cc/8SSR-PGLJ] (last visited June 1, 2015).

51 Anti-Counterfeiting Trade Agreement art. 27.5-27.7, Jan. 1, 2011, 50 I.L.M. 243.

52 *Id.* art. 27.2-27.4.

53 *Pirate Parties: From Digital Rights to Political Power*, BBC NEWS TECHNOLOGY (Oct. 18, 2011), http://www.bbc.com/news/technology-15288907 [http://perma.cc/T7LG-VMCY].

54 *See generally* PATRICK BURKART, PIRATE POLITICS: THE NEW INFORMATION POLICY CONTESTS 1 (2014).

55 *Id.* at 1-2.

56 Ernesto, *Pirate Party Wins and Enters the European Parliament*, TORRENTFREAK (June 7, 2009), https://torrentfreak.com/pirate-party-wins-and-enters-the-european-parliament-090607 [https://perma.cc/5M44-EH6R].

57 Nicholas Kulish, *Pirates' Strong Showing in Berlin Elections Surprises Even Them*, N.Y. TIMES (Sept. 19, 2011), http://www.nytimes.com/2011/09/20/world/europe/in-berlin-pirates-win-8-9-percent-of-vote-in-regional-races.html [http://perma.cc/2K38-RHZV].

briefly became Germany's "third-most-popular party,"[58] and elected approximately two hundred and fifty candidates worldwide.[59] Pirates see their name not as a reference to illegality but rather as the re-appropriation of a term that they believe rights holder representatives wrongly applied to Internet users.[60]

Press representations denigrated the Pirate movement as a product of social disaffection whose politicians entered easy-to-infiltrate parliamentary coalitions via protest votes.[61] But this criticism misses a broader perspective. Pirates represent a particularly technologically well-informed citizens movement that gained political influence despite press disparagement. The intellectual history behind their platforms reveals that they manifest, and make popularly accessible, deep conflicts within existing intellectual property regimes. Indeed, Pirates have translated these complex issues and circulated them effectively in media-friendly form. Hence, they offer an opportunity to observe how pro-privacy arguments for DRM reform can play out in contested political domains.

Most Pirates seek to legalize DRM circumvention and either limit or prohibit the use of DRM altogether.[62] For instance, the copyright reform platform developed by current pirate Member of the European Parliament Christian Engström—and later adopted by the Greens and European Free Alliance within the Parliament—reads: "It must always be legal to circumvent DRM restrictions, and we should consider introducing a ban in the consumer rights legislation on DRM technologies that restrict legal uses of a work."[63] The Uppsala Declaration, a joint policy statement of pirate parties

---

[58] Steven Kettmann, *New Politics, Ahoy!*, N.Y. TIMES (May 2, 2012), http://www.nytimes.com/2012/05/02/opinion/the-pirate-party-logs-a-new-politics.html [http://perma.cc/XX9T-FT8K].

[59] MOZART OLBRYCHT-PALMER, SUBMISSION TO THE ATTORNEY-GENERAL'S DEPARTMENT ON THE REVIEW OF TECHNOLOGICAL PROTECTION MEASURE EXCEPTIONS MADE UNDER THE COPYRIGHT ACT 1968 (2012), https://www.ag.gov.au/RightsAndProtections/IntellectualProperty/CurrentIssuesReformsandReviews/Documents/PiratePartyAustraliaSubmission.pdf.

[60] *E.g.*, Jolly Anonymous Roger, *About the PPI*, PP INT'L (Dec. 30, 2009), http://pp-international.net/about [http://perma.cc/8YXK-5HKA].

[61] *See, e.g.*, Stephen Castle, *Disaffection Dominates European Voting*, N.Y. TIMES (June 7, 2009) http://www.nytimes.com/2009/06/08/world/europe/08union.html [http://perma.cc/Q86Y-EJP6]; Sally McGrane, *Idea of 'One Person One Party' Makes for a Crowd in Switzerland*, N.Y. TIMES (Sept. 21, 2011), http://www.nytimes.com/2011/09/22/world/europe/political-parties-on-fringe-abound-in-switzerland.html [http://perma.cc/VZ3R-PB2L].

[62] CHRISTIAN ENGSTRÖM MEP & RICK FALKVINGE, THE CASE FOR COPYRIGHT REFORM 6 (2012).

[63] *Id.*

throughout Europe, demands that DRM be "outlawed."[64] The Swedish party wants it "banned,"[65] and the German pirates call for "no (technical) restrictions on copying."[66]

To support these platforms, Pirates have drawn repeatedly on pro-privacy arguments. The German Pirate Manifesto, for instance, warns that DRM makes it "possible to control and monitor users in completely inacceptable ways."[67] Even those Pirates who favor more modest proposals to limit rather than ban DRM make pro-privacy arguments. The U.K. Pirate Party has endorsed the "right to private and confidential communication," and promised to "ensure that the freedom to encrypt data and communications is not abridged or limited and that access to the tools that make secure communications easier is not restricted."[68] Perhaps for this reason, the Party would restrict but not prohibit DRM.[69] After all, complete bans on DRM could adversely affect other uses of encryption—including use for confidential communication. Other Pirates promote mandatory consumer protection warnings for products that incorporate DRM.[70] These platforms also gain support from pro-privacy rhetoric. Swedish party proposals that "any product containing DRM shall display clear warnings"[71] match U.K. Pirate beliefs that consumers need protection from "products that 'phone home.'"[72]

Some Pirates argue further that any enforcement of copyright laws in the digital age necessarily threatens privacy. Engström prefaced his copyright reform platform with the

---

64 *European Pirate Platform 2009 The Uppsala Declaration*, NYHETER FRÅN GAMLA PIRATPARTIET.SE (July 2, 2008), http://historik.piratpartiet.se/?p=933 [http://perma.cc/G2WK-D5JN].

65 PIRATE PARTY SWEDEN, PIRATE PARTY DECLARATION OF PRINCIPLES/3.2/FREE OUR CULTURE 3, http://en.wikisource.org/wiki/Pirate_Party_Declaration_of_Principles/3.2/Free_Our_Culture [http://perma.cc/Z4QR-6NGL] (last visited May 10, 2014).

66 EMAL GHAMSHARIK & JULIA REDA, MANIFESTO OF THE PIRATE PARTY OF GERMANY ENGLISH VERSION 6 (2012), http://www.piratenpartei.de [http://perma.cc/6WDP-CAND].

67 *Id.* at 6.

68 *Respect Privacy*, PIRATE PARTY UK, http://policy.pirateparty.org.uk/policy/civil-liberties/respect-privacy [http://perma.cc/8LGY-GE3S] (last visited Apr. 15, 2015).

69 *Digital Accessibility*, PIRATE PARTY UK, http://www.ppuk.org.uk/policy/social-policy/digital-accessibility [http://perma.cc/EF86-EN2J] (last visited Apr. 15, 2015).

70 PIRATE PARTY SWEDEN, PIRATE PARTY DECLARATION OF PRINCIPLES 3.2, at 3 (2008), http://docs.piratpartiet.se/Principles%203.2.pdf [http://perma.cc/2G58-SYHG].

71 *Id.*

72 *Limit Digital Rights*, PIRATE PARTY UK, http://www.ppuk.org.uk/policy/digital-economy-and-digital-rights/limit-digital-rights-management [http://perma.cc/5MHA-G6S3] (last visited Apr. 15, 2015).

observation that "copyright enforcement threatens fundamental rights, including the right to private communication."[73] Engström and Rick Falkvinge, the founder of the first Swedish Pirate Party, have proposed to legalize DRM circumvention and ban any DRM that interferes with non-infringing uses of copyrighted materials.[74] "Today's level of copyright cannot coexist with the right to communicate in private," they wrote in a co-authored book about copyright reform.[75] "We, as a society, can say that copyright is the most important thing we have, and give up the right to talk in private. Either that, or we say that the right to private correspondence has greater value, even though such correspondence can be used to transfer copyrighted works."[76] Falkvinge summed up on Twitter: "[y]ou cannot enforce the copyright monopoly without mass surveillance of people's private communications. Therefore, the monopoly must go."[77]

The Pirates may mean at least three things by these statements. First, unlike the analogue world where material constraints on duplication permit rights holders to focus their enforcement efforts on the first sale in a distribution chain, the near infinite capacity to copy digital content online encourages rights holders to monitor every point of distribution and consumption—necessarily invading privacy. Second, as Amy Kapczynski has explained, markets for copyrighted content create inherent tensions between privacy and sellers' incentives to price discriminate, which are in turn exacerbated by the ease of tracking consumers online.[78] Third, Falkvinge's statement evokes the broad deregulatory valence of privacy rights, which wall off space from state intrusion.[79] The implications of this later claim are hard to overstate. Similar logic could apply to most any law restricting the free flow of information on the Internet. To enforce laws about information access and use necessarily invades privacy because, practically speaking, it requires some form of monitoring.

III. Privacy Claims and Counterclaims in the DRM Debates

---

[73] ENGSTRÖM & FALKVINGE, *supra* note 62, at 7.

[74] *Id.* at 6.

[75] *Id.* at 8.

[76] *Id.* at 9.

[77] Rick Falkvinge (@Falkvinge), TWITTER (Apr. 12, 2014, 5:35 AM), https://twitter.com/Falkvinge/status/454930790460448768 [https://perma.cc/3BRP-UAHM].

[78] Amy Kapczynski, *The Cost of Price: Why and How to get Beyond Intellectual Property Internalism*, 59 UCLA L. REV. 970, 1016 (2012).

[79] *See, e.g.*, Reva B. Siegel, "*The Rule of Love": Wife Beating as Prerogative and Privacy*, 105 YALE L.J. 2117, 2153, 2173 (1996) (tracing the history of "privacy as a justification for chastisement" and noting feminist "efforts to pierce the veil of privacy talk around the practice" of martial violence).

A series of legal arguments, most prominently initiated by Julie Cohen and hashed out in longstanding scholarly debates, support many if not all of Pirate politicians' pro-privacy claims for DRM reform.[80] To be sure, most of these arguments remain untested. In U.S. courts, the sparse privacy claims that have been raised against DRM have generally failed.[81] Still, their theoretical development in a robust body of legal scholarship lends credence to Pirate party platforms and similar reform efforts.

Yet historically, rights holder representatives and others made similar pro-privacy arguments to support the widespread adoption of DRM and anti-circumvention laws in the first place.

For instance, rights holder representatives in both WIPO forums and U.S. congressional hearings argued that DRM technologies themselves offer the best protection for privacy against the very threats these technologies impose. At a 1998 session of the WIPO Advisory Committee on the Management of Copyright and Related Rights, rights holder representatives circulated a report that acknowledged privacy issues with DRM and then offered better-calibrated DRM as the solution to those

---

[80] Cohen has been arguing for approximately two decades that DRM threatens information privacy. As early as 1996, she identified a First Amendment "right to read anonymously." As a result, she suggested that anti-circumvention laws that restrict users from bypassing DRM might be unconstitutional. Cohen, *A Right to Read Anonymously*, *supra* note 4, at 1029. ("[A]nti-tampering provisions . . . encompass conduct protected by the First Amendment and, if enacted, cannot constitutionally be enforced against individuals who exercise technological self-help to protect their freedom to read anonymously."). Again in 1997, she cautioned that, "[DRM] capabilities . . . threaten individual privacy to an unprecedented degree." Julie E. Cohen, *Some Reflections on Copyright Management Systems and Laws Designed to Protect Them*, 12 BERKELEY TECH. L.J. 161, 184 (1997). And in 2003 she developed a multi-factored framework to show precisely how "DRM technologies are poised to affect both the spatial and the informational dimensions of intellectual privacy." *See, e.g.*, Cohen, *DRM and Privacy*, *supra* note 20, at 580; s*ee also*, Julie E. Cohen, *Copyright and the Jurisprudence of Self-Help*, 13 BERKELEY TECH. L.J. 1089 (1998). For other scholars who have argued a similar perspective, see Lilian Edwards, *Coding Privacy*, 84 CHI.-KENT L. REV. 861, 869 (2010) (commenting on the privacy-invasive code in the "Sony DRM rootkit"); Sonia K. Katyal, *The New Surveillance*, 54 CASE W. RES. L. REV. 297, 351 (2003) (arguing that DRM "is another kind of piracy surveillance . . . ."); and Neil M. Richards, *The Information Privacy Law Project*, 94 GEO. L.J. 1087, 1116-17 (2006) (describing the scholarly debate about privacy, speech, and DRM).

[81] *See, e.g.*, Cunningham v. McMahon, 2008 WL 829107, at *2 (S.D.W. Va., Mar. 27, 2008) (dismissing a claim that Apple invades privacy by using DRM to place licenses on the computers of its customers).

same issues.[82] In their words, DRM "does not in and by itself protect privacy. But it is probably the best tool to do so."[83]

As with Pirate rhetoric, rights holder claims about DRM and privacy find deeper theoretical support. Judges and legal scholars both have endorsed the pro-privacy pro-DRM perspective. While the majority of DMCA Section 1201 litigation has addressed alternate issues like fair use,[84] the reach of the anti-circumvention prohibitions, [85] or interoperability,[86] judges who have weighed in on privacy in even a small way have credited DRM as privacy enhancing.[87]

This Part documents how advocates both for and against DRM and anti-circumvention laws have made claims on informational privacy, and categorizes these claims according to the deeper conceptions of privacy that each implies. It presents a summary of Cohen's pro-privacy claims and those of other anti-DRM advocates. It also draws on the diplomatic histories of the WIPO Copyright Treaty and the WIPO Performances and Phonograms Treaty and on the legislative history of the DMCA to show how pro-privacy arguments have bolstered legal protections for DRM over time.[88]

A. Privacy as Property

Many of today's ongoing pro-privacy anti-DRM reform efforts focus on market failures and posit forms of consumer protection as likely remedies.[89] These consumer protection claims imply that informational privacy is a form of property in at least two different ways. First, some advocates allege that

---

[82] *Id.* at 4, 11. For clarity, I refer to DRM in my discussion of this study. However, the paper itself uses the term ECMS and not DRM. Technical differences between the two are not relevant to this discussion.

[83] DANIEL J. GERVAIS, ELECTRONIC RIGHTS MANAGEMENT AND DIGITAL IDENTIFIER SYSTEMS 29 (1998) http://www.wipo.int/meetings/en/details.jsp?meeting_id=3646 [http://perma.cc/JKB3-VGX5].

[84] *See, e.g.*, Chamberlain Group, Inc. v. Skylink Technologies, Inc., 381 F.3d 1178, 1196 (Fed. Cir. 2004); Universal Studios, Inc. v. Corley, 273 F.3d 429, 443 (2d Cir. 2001).

[85] *See, e.g.*, MGE UPS Sys., Inc. v. GE Consumer & Indus., Inc., 622 F.3d 361, 366 (5th Cir. 2010).

[86] Universal City Studios v. Reimerdes, 111 F. Supp. 2d 294, 320 (2d Cir. 2001).

[87] In *United States v. Reichart*, for example, a dissenting judge on the Sixth Circuit described DRM as a technology that manufacturers use "to strengthen privacy controls." United States v. Reichart, 747 F.3d 445, 456 (6th Cir. 2014).

[88] MIHÁLY FICSOR, THE LAW OF COPYRIGHT AND THE INTERNET: THE 1996 WIPO TREATIES, THEIR INTERPRETATION AND IMPLEMENTATION 359 (2002).

[89] These anti-DRM arguments are reminiscent of James Grimmelmann's suggestion that some information privacy issues are analogous to those of product safety law. James Grimmelmann, *Privacy as Product Safety*, 19 WIDENER L.J. 793, 813-23 (2010).

sellers insufficiently disclose the DRM in their products. Sellers may fail adequately to notify consumers about DRM technologies that collect more information than necessary to transact a sale or guarantee a product function, or that access and share personal information with third parties without consumer knowledge or consent.[90] These allegations suggest that if only consumers were to receive better notice, their choices to sell their personal information would more faithfully reveal their actual preferences. In other words, informational privacy is a good that can and even should be transacted, just in markets better than those we currently have.

Second, other anti-DRM advocates have argued that consumers purchase the right to engage privately with a digital product when they buy that product. Consumers who are unable to control information about how they engage with a product are not owners but mere lessees. Engineer Paul Sweazey, who devised an IEEE Standards Association proposal to reform DRM so as to make consumer ownership of digital content products more similar to that of physical goods, exemplifies this perspective.[91] Sweazey considers privacy to be an attribute of ownership,[92] and blames online copyright violations on "a cyberspace marketplace that denies the fulfillment of basic human needs (the autonomy and privacy of personal property)."[93]

At the same time, pro-privacy pro-DRM advocates have used a privacy-as-property perspective to help justify the widespread adoption of DRM and legal bulwarks to protect it. In WIPO forums during the 1990s, rights holder representatives claimed that it was rights holders' own privacy

---

[90] *Digital Content Products*, *supra* note 23, at 15. In one notorious case, Sony BMG sold music CDs with a DRM software called MediaMax that installed on consumers' computers without their consent and transmitted information about their listening habits to a corporation called SunnComm. The MediaMax DRM collected this information despite the fact that Sony's Licensing Agreement and the SunnComm website both wrongly stated that consumers' personal information would not be collected. *Sony BMG Litigation Info*, ELEC. FRONTIER FOUND., https://www.eff.org/cases/sony-bmg-litigation-info [https://perma.cc/2Y37-NGKZ] (last visited April 15, 2015). After investigations from several state and federal government authorities, class action lawsuits in New York and California, and a lawsuit brought by the Texas Attorney General, Sony BMG ultimately recalled the CDs. *See, e.g.*, Motion and Memorandum of Law in Support of Plaintiffs' Application for Preliminary Approval of Class Action Settlement at 1, 7, In re SONY BMG CD Technologies Litigation, No 05-09575-NRB (S.D.N.Y. Dec. 28, 2005), *available at* https://www.eff.org/document/motion-preliminary-approval-sony-bmg-settlement [https://perma.cc/Q9SF-9SYQ].

[91] Paul Sweazey, *Introduction to Digital Personal Property*, *in* CONSUMERS IN THE INFORMATION SOCIETY: ACCESS, FAIRNESS AND REPRESENTATION 53-71 (Jeremy Malcolm ed., 2012).

[92] *Id*. at 55, 64.

[93] *Id*. at 70.

interests—not those of consumers—that were at stake. This position starts with the perspective that copyright merely expresses a property-based concept of informational privacy. Because both copyright and privacy interests justify restricting access to information, the property right in copyrighted information can be interchanged with a privacy interest in that same information.

A 1993 WIPO symposium, the first of a series of brainstorming meetings that the organization hosted prior to enacting the WIPO Copyright Treaty and WIPO Performances and Phonograms Treaty, exemplifies this view.[94] Paul Geller, a professor of intellectual property law who presented at the symposium, argued that rights holders could deploy DRM technologies to secure their own communicative privacy. He advised rights holders to use DRM to limit access to select audiences, rather than distributing their content in open public channels such as television or radio broadcasts. Geller reasoned that by using encryption to transmit the content only to a select group of consumers, rights holders could maintain a legally cognizable interest in the confidentiality of that content.[95] With encryption (or DRM), he argued, "reliance [would shift] from copyright . . . to privacy," and that "[o]riginators of works and other media productions could stand on their privacy rights to restrict access."[96] With DRM, privacy rights could supplant copyright altogether.[97]

B. Spatial Privacy

Julie Cohen has argued that DRM violates spatial concepts of information privacy when these technologies track user consumption in certain physical locations, specifically those where individuals reasonably expect not to be observed such as

---

94 FICSOR, *supra* note 88, at 29-32.

95 WORLD INTELLECTUAL PROP. ORG., WIPO WORLDWIDE SYMPOSIUM ON THE IMPACT OF DIGITAL TECHNOLOGY ON COPYRIGHT AND NEIGHBORING RIGHTS 217 (WIPO, Publication No. 723 (E), 1993), *available at* https://perma.cc/7Z3K-GJPM.

96 Geller reasoned that copyright would remain relevant only as a "stop-gap" measure in case DRM protections were "not adequately policed." *Id.* at 217-18.

97 Geller's arguments dominated the symposium discussion of privacy issues. Technologist Ashok Bhojwani gestured towards concern that privacy-driven restrictions on access could hinder international development. *Id.* at 88. But the only direct counterargument to Geller was a brief caution by Arthur Miller, a professor of copyright and privacy law, that "encryption, metering, and surveillance of use pose enormous threats to personal privacy." *Id.* at 244. To assuage concerns, Geller assured that disaggregating the control of information could protect "the privacy rights of all parties communicating," hinting at yet another DRM solution to DRM problems. *Id.* at 218.

the home.[98] In these cases, she reasons that the privacy tort of Intrusion Upon Seclusion should cover DRM.[99] Intrusion Upon Seclusion protects against invasions of privacy "that would be highly offensive to a reasonable [person]."[100] Of course, what counts as "offensive" fluctuates; fewer reasonable persons today may take offense to DRM tracking inside homes that also house eavesdropping TV's. Yet because privacy interests are generally recognized to increase inside homes, these spaces offer a relatively strong chance at privacy protection.

However, spatial concepts of information privacy—and especially privacy interests inside the home—also provided an historic rationale for fortifying DRM with anti-circumvention laws. This pro-privacy argument applies specifically to bans on trafficking in circumvention devices. The argument is that these bans enable remote enforcement via the public marketplace and thereby obviate the need for law enforcement intrusions into traditionally private spaces such as the home. Here, the idea is not precisely that DRM technologies are independently privacy enhancing, but rather that expansive legal bulwarks for DRM technologies create a more privacy protective alternative than other forms of copyright enforcement.

A 1999 WIPO-run workshop on implementing the WIPO Copyright Treaty into national domestic laws demonstrates this perspective. Workshop participants cited privacy as reason to expand the treaty's prohibitions to the manufacture and distribution of circumvention devices. Recall that, unlike the DMCA, the WIPO treaties merely require "effective legal remedies" against circumvention.[101] The workshop participants observed that the physical act of disabling DRM "is usually private."[102] The mandated "effective legal remedies" could thus potentially require law enforcement to invade homes and workplaces to target the act of circumvention.[103] Yet, the workshop concluded that it is "neither feasible nor desirable to undertake systematic monitoring of private conduct to deter circumvention activity."[104] Greater ex ante constraints on

---

98 Cohen, *DRM and Privacy*, *supra* note 20, at 585.

99 *Id.* at 591-95.

100 RESTATEMENT (SECOND) OF TORTS § 652B (1977).

101 *Id.* at 11.

102 DEAN S. MARKS & BRUCE H. TURNBULL, WIPO WORKSHOP ON IMPLEMENTATION ISSUES OF THE WIPO COPYRIGHT TREATY (WCT) AND THE WIPO PERFORMANCES AND PHONOGRAMS TREATY (WPPT), TECHNICAL PROTECTION MEASURE: THE INTERSECTION OF TECHNOLOGY, LAW AND COMMERCIAL LICENSES 6 (Dec. 3, 1999), *available at* http://www.wipo.int/edocs/mdocs/copyright/en/wct_wppt_imp/wct_wppt_imp_3.pdf [http://perma.cc/KHR2-PTYY].

103 *Id.*

104 *Id.*

behavior could alleviate these intrusions.[105] Countries would thus reduce law enforcement threats to spatial privacy by implementing the WIPO Copyright treaty expansively to prohibit not merely acts of circumvention but also the services and devices that facilitate them.[106]

C. Contextual Privacy

Other anti-tracking arguments against DRM pin privacy protections to particular uses of information, or to specific communicative relationships. For instance, Cohen notes that content providers sometimes use data collected through DRM not to enforce copyright but rather to enhance their profiles of users' intellectual preferences and consumption habits—a process she finds more comprehensive and thus more invasive than traditional consumer profiling.[107] Cohen argues that content providers create "second-order privacy effects" when they monetize these enhanced profiles or sell them to third parties.[108] In other words, the information warrants protection from alternate uses and further distribution. Her claim thus implies that the information generated by DRM tracking acquires some type of privacy interest that is unique to the relationship within which the information was generated—in this case a provider-consumer transaction.

An implied definition of privacy that tracks uses of information or communicative relationships also helps to explain another of Cohen's concerns; even fully automated DRM data collection threatens privacy. Information collected by automated processes is still "subject to disclosure or compelled production," she has argued, so collecting it can "chill intellectual exploration, and therefore compromise intellectual privacy interests."[109] In other words, the threat of disclosure—even if it fails to materialize—creates a chilling effect similar to the knowledge of present monitoring.[110]

---

[105] Cohen comments of this argument: "This strategy subverts the logic of privacy-as-inaccessibility . . . the feasible uses of the CD are known, and so the question of particularized accessibility to me is moot." Cohen, *DRM and Privacy*, *supra* note 20, at 582.

[106] MARKS & TURNBULL, *supra* note 102, at 6. Marks and Turnbull explicitly credit their interpretation of the WIPO Copyright Treaty to the "DMCA's concepts and solutions," which prohibits circumvention devices as well as conduct. *Id.*; s*ee also*, Digital Millennium Copyright Act of 1998, 17 U.S.C. § 1201 (a)(2)(A) (2012) (prohibiting "any technology, product, service, device, component, or part thereof, that is primarily designed or produced for the purpose of circumventing a technological measure").

[107] Cohen, *DRM and Privacy*, *supra* note 20, at 586.

[108] *Id.* at 585-86.

[109] *Id.* at 585.

[110] To be sure, the threat of downstream disclosure applies to lots of data collection. RadioShack, for example, recently tried to sell consumer information in violation of its own former privacy policy when it filed for

Indeed, the pervasive risk of security breaches and theft means that information about consumers' intellectual activities may become accessible not just to any third party but to criminal intruders or even the public at large.[111] It is important to note that the privacy interest at stake in all these instances covers information collected for a particular use in a specific communicative relationship, and a violation of that interest occurs whenever the information moves beyond its initial context.

Yet contextual understandings of information privacy—i.e., privacy interests tied to specific uses of information or to particular relationships between communicating parties—also appear in pro-DRM claims. These arguments play out most easily for DRM access controls. Like other forms of encryption, DRM access controls can restrict disclosure, [112] mitigate leaks,[113] and prevent surveillance.[114] Access controls can thus

---

bankruptcy in February 2015, prompting a complaint from the Texas Attorney General. *See, e.g.*, Andrea Peterson, *Bankrupt RadioShack Wants to Sell Off User Data. But the Bigger Risk Is if a Facebook or Google Goes Bust*, Wash. Post, Mar. 26 2015, http://www.washingtonpost.com/blogs/the-switch/wp/2015/03/26/bankrupt-radioshack-wants-to-sell-off-user-data-but-the-bigger-risk-is-if-a-facebook-or-google-goes-bust [https://perma.cc/WF2H-C3YL]. But DRM tracking stands out because anti-circumvention legislation protects this form of commercial monitoring above and beyond more common contractual obligations.

[111] For instance, in addition to collecting information, the MediaMax DRM also introduced security vulnerabilities into users' computers that increased their susceptibility to direct attacks by third party malware. *Sony BMG Litigation Info*, *supra* note 90.

[112] Jonathan Zittrain argued as early as 1999 that the same DRM technologies copyright owners had developed to fight piracy could benefit medical privacy; DRM could supplement potentially insufficient legal protections for the confidentiality of medical records. Jonathan Zittrain, *What the Publisher Can Teach the Patient: IP and Privacy in an Era of Trusted Privication*, 52 STAN. L. REV. 1200, 1201 (2000) ("Those who worry about the confidentiality of medical records might seek to augment comparatively paltry legal protections with [DRM].").

[113] Some vendors advertise their DRM products specifically as means to protect sensitive documents from leaks. If those sensitive documents include consumer profiles, DRM-enhanced security would accrue to the privacy interests of the individuals they represent. *See, e.g.*, Yuval Shavit, *Data Security: Alternatives to Data Leak Prevention*, SEARCHITCHANNEL (Mar. 2008), http://searchitchannel.techtarget.com/feature/Data-security-Alternatives-to-data-leak-prevention [http://perma.cc/85ST-Y24A] (last visited Sept. 27, 2015) ("DRM software recognizes when a portion of [a sensitive] file is copied, encrypted or otherwise embedded into another file . . . allowing the software to monitor or block its transmission . . . .").

[114] Recently, technology researchers have suggested that incorporating DRM into digital photographs would protect against "surveillance by governmental agencies and scandalous leakage of private photos." Mike Masnick, *JPEG Looking to Add DRM to Images . . . Supposedly to Protect Images from Gov't Surveillance*, TECHDIRT (Jul. 15, 2015, 11:38AM), https://www.techdirt.com/articles/20150714/06503331631/jpeg-looking-to-

empower individuals to restrict their personal information to particular uses or specific communicative relationships. In other words, DRM can actually reduce the risk of Cohen's "second-order privacy effects," including the threat of disclosure and the intellectual chilling effect that disclosure produces.[115]

Somewhat less intuitive, others have argued that even DRM direct tracking and the punitive use of access controls can protect contextual and relationship-based privacy interests. For a recent instantiation of this claim, Jerry Kang and co-authors proposed in 2012 to ameliorate information privacy issues with a technological self-help measure called "Privacy Rights Management ('PRM')."[116] PRM—a form of DRM for privacy—would empower a new class of professional data intermediaries to monitor the use of personal data by third parties and to revoke access in the case of wrongdoing or unauthorized use. It could also permit the individuals who originated the personal information to delete the data remotely if they changed their opinion about having shared it.[117] In short, in this view, if DRM technologies are in the hands of users or consumers or their agents, their tracking and punitive targeting capacities will help to control downstream disclosure of private information.

D. Privacy as Anonymity

To argue against rights holders' use of access controls to punish individual users for alleged violations of copyright law or contract, Cohen claims that the practice threatens privacy because it de-anonymizes individuals from the mass of other users.[118] As a recent example, in 2012 Amazon remotely deleted the entire Kindle library of a Norwegian IT consultant named Lynn Nygaard.[119] The company offered neither notice nor explanation beyond its terms of use agreement: "In case of [failure to comply with the agreement], Amazon may immediately revoke your access to the Kindle store and the

---

add-drm-to-images-supposedly-to-protect-images-govt-surveillance.shtml [https://perma.cc/KW3J-LAE3].

[115] Zittrain called DRM systems the "coupling of mass distribution of information to 'authorized' users with tight control over its use." Zittrain, *supra* note 112, at 1218.

[116] Jerry Kang et al., *Self-Surveillance Privacy*, 97 IOWA L. REV. 809, 844 (2012).

[117] This process, termed "remote revocation" by the authors, bears striking resemblance to the Nygaard Kindle library fiasco. *Id.; see also infra* notes 126-26 and accompanying text.

[118] Cohen, *DRM and Privacy*, *supra* note 20, at 587.

[119] Mat Honan, *Remote Wipe of Customer's Kindle Highlights Perils of DRM (Updated)*, WIRED (Oct. 22, 2012, 4:39PM), http://www.wired.com/2012/10/amazons-remote-wipe-of-customers-kindle-highlights-perils-of-drm [http://perma.cc/ZYZ3-USAW].

Kindle Content."[120] After Nygaard's story caught the attention of the blogosphere, Amazon restored her library with no further comment. [121] Applying Cohen's argument to Nygaard's situation, Amazon violated her privacy by singling her out inappropriately from others who were similarly situated. The argument implies that information privacy incorporates a privacy interest in remaining undifferentiated from one's peers—a form of anonymity-as-privacy that invokes due process values of treating like alike.

Once again, privacy-as-anonymity makes an appearance in pro-DRM claims as well. In a reverse of Cohen's argument about punitive targeting, rights holder representatives at the 1998 WIPO Advisory Committee session suggested that intermediaries could use DRM both to collect information and also to anonymize it.[122] DRM technologies that "aggregate data so as to protect privacy and confidentiality," the report concluded, "are probably essential ingredients of the success (or failure) of electronic copyright commerce."[123] The implication here is that data aggregation can further information privacy interests because it creates the exact opposite process from the de-anonymization that Cohen fears; data aggregation forces the treatment of individuals as an undifferentiated mass.

E. Substantive Privacy

Cohen draws on a substantive concept of information privacy to argue against DRM access controls. [124] Usage constraints, she points out, reduce individuals' capacity to make choices about their "intellectual consumption" free from external interference. [125] This argument echoes substantive privacy concerns about state interference with important decisions, and as well Richards' concept of "intellectual privacy" protections against external intrusion in the formation of ideas. DRM access controls limit intellectual choices and thereby invade a personal autonomy component of information privacy.

Similarly, rights holder representatives in U.S. congressional hearings invoked substantive concepts of

---

[120] *Id.* (quoting *Help & Customer Service, Kindle Store Terms of Use*, AMAZON.COM (Sept. 6, 2012) http://www.amazon.com/gp/help/customer/display.html?nodeId=201014950 [http://perma.cc/DP7R-Y6S4]).

[121] Michelle Jaworski, *Amazon Restores Kindle User's Mysteriously-Deleted Account, Still No Explanation*, THE DAILY DOT (Oct. 23, 2012, 12:54 PM), http://www.dailydot.com/news/amazon-linn-nygaard-deleted-account-restored [http://perma.cc/7PCB-HPNS].

[122] *Id.* at 29 ("The rights holder thus gets necessary market data without any risk of confidentiality or privacy violation.").

[123] *Id.* at 30.

[124] Cohen, *DRM and Privacy*, *supra* note 20, at 580-82.

[125] *Id.* at 580, 582.

information privacy to argue in favor of DRM. Consider the idea that copyright reflects an interest in cognitive and decisional autonomy free from external interference. The representative of a U.S. e-commerce company introduced something similar to this perspective at a 2001 House committee hearing on information privacy. "In our view, privacy, intellectual property, and copyright protection are all critical aspects of the same common issue," he testified. "[Securing digital assets with DRM] is equivalent to defending personal and potentially national integrity."[126] This claim that using DRM to protect copyrighted information is "equivalent" to defending personal integrity primarily invokes data security concerns. Yet recall that better data security is also a remedy for the risk of disclosure, a risk that—as Cohen argued—can chill intellectual exploration, impair decisional autonomy, and threaten substantive privacy.

While hardly central in U.S. jurisprudence, a substantive privacy interest in copyrighted information is not entirely without theoretical support. In their foundational text defining privacy as the right "to be let alone," Warren and Brandeis argued that "the legal doctrines relating to infractions of what is ordinarily termed the common-law right to intellectual and artistic property are, it is believed, but instances and applications of a general right to privacy."[127] In other words, intellectual property rights that were asserted successfully at common law to prevent the publication of a literary work, such as a personal letter, reflected an underlying privacy interest.[128] Jane Ginsburg has more recently echoed this claim by arguing that both common law copyright and privacy rights arose from the same "rights of personality."[129]

F. Material Privacy

Finally, arguments on both sides of the DRM debates hint at an underexplored concept that warrants further consideration: information privacy as a material interest.[130]

This concept is visible in debates over anti-circumvention laws. Like the supporters of such laws, their doppelganger

---

[126] *Information Privacy: Industry Best Practices and Technological Solutions: Hearing Before the Subcomm. on Commerce, Trade, & Consumer Protection of the H. Comm. On Energy & Commerce*, 107th Cong. 32 (2001) (statement of John Schwarz, CEO Reciprocal).

[127] Warren & Brandeis, *supra* note 11, at 198.

[128] *Id.* at 200-01.

[129] Jane C. Ginsburg, *Creation and Commercial Value: Copyright Protection of Works of Information*, 90 COLUM. L. REV. 1865, 1883 (1990).

[130] For a helpful examination of the relationship between material privilege and privacy rights, see Akhil Reed Amar, *America's Lived Constitution*, 120 YALE L.J. 1734, 1770 (2011).

critics focus on trafficking in circumvention devices. The DMCA exempts acts of circumvention undertaken solely to protect personally identifiable information.[131] But anti-DRM critics have argued that Section 1201 renders this exception moot because it prohibits not merely the act or conduct of circumvention but also the manufacture and distribution of circumvention devices. [132] As a result, the exemption is practically available only to the limited number of individuals with the skills to engineer such devices themselves.[133] Indeed, I would add that the exemption exacerbates the technological literacy barrier still further because it applies only to DRM that collects personally identifiable information "without providing conspicuous notice of such collection"—meaning users must have the skills to discover that collection independently—and because it permits only those acts of circumvention that disable information collection with "no other effect" on access—throwing an additional burden on the engineering of circumvention tools.[134] In sum, then, expanding anti-circumvention provisions from conduct to devices effectively eliminates whatever minimal privacy protections the DMCA would otherwise have provided. The deeper implication here is that legal protections for privacy are insufficient unless they also enable access to the material resources necessary to assert those interests.

On the other hand, advocates for DRM in both WIPO forums and the U.S. Senate Judiciary Committee invoked a material concept of privacy to defend anti-circumvention laws. Their argument was simple; because DRM protects privacy, laws that protect DRM also protect privacy. Legal

---

[131] Section 1201(i). For an excellent analysis of the legislative discussions that led to this exemption, see Bill D. Herman & Oscar H. Gandy, Jr., *Catch 1201: A Legislative History and Content Analysis of the DMCA Exemption Proceedings*, 24 CARDOZO ARTS & ENT. L.J. 121(2006), and Pamela Samuelson, *IP and the Digital Economy: Why the Anti-Circumvention Regulations Need to Be Revised*, 14 BERKELEY TECH. L.J. 519, 542 (1999).

[132] Section 1201(a)(2).

[133] *See, e.g.*, *Anticircumvention (DMCA)*, CHILLING EFFECTS, https://www.chillingeffects.org/anticircumvention/faq.cgi#QID119 [https://perma.cc/Q24W-S844] (last visited April 15, 2015) (arguing that the DMCA's ban on circumvention devices leaves the personal privacy exemption available only to those with the skills "to analyze and manipulate computer source code in order to protect their privacy . . . ."). Indeed, I would add that the exemption exacerbates the technological literacy barrier still further because it applies only to DRM that collects personally identifiable information "without providing conspicuous notice of such collection," meaning users must have the skills to discover that collection independently, and because it permits only those acts of circumvention that disable information collection with "no other effect" on access, throwing an additional burden on the engineering of circumvention tools. § 1201(i)(B)-(C).

[134] § 1201(i)(B)-(C).

enhancements for DRM will bolster whatever function the technology already performs. Of course, as the above discussion has hopefully made clear, precisely what function DRM performs is ambiguous. Nonetheless, advocates argued that anti-circumvention laws would strengthen DRM in general. Bolstering DRM in all instances—including when DRM controls information that otherwise appears removed from privacy issues—would create spillover effects to strengthen its privacy-enhancing capacity when needed. This spillover effect applies both to the anti-circumvention bans and to the prohibition on trafficking in circumvention devices. As the Senate Judiciary Committee Report on the DMCA emphasized:

> [S]ection 1201 should have a positive impact on the protection of personal privacy on the Internet. The same technologies that copyright owners use to control access to and use of their works can and will be used to protect the personal privacy of Internet users . . . By outlawing the activities of those who make it their business to provide the tools for circumventing these protective technologies, this legislation will substantially enhance the degree to which individuals may protect their privacy.[135]

In other words, one way to protect privacy is by protecting the materials that enhance it, regardless of whether they are applied to privacy concerns in any given instance.

IV. Explanations

The above Parts show that advocates on conflicting sides of the DRM debates have deployed corresponding privacy-based arguments to justify opposing policy preferences. These competing claims on privacy are not limited to superficial struggles over common terms, but rather concern a variety of deeper conceptions of privacy interests. Claims on property-based, spatial, contextual, anonymity-based, substantive, and material understandings of information privacy each correspond to counterclaims on those same interests.

One possible explanation for these observations is that privacy claims are unstable simply because they are a type of rights claim. From this perspective, the DRM debates are an instance of a much larger phenomenon: the broader indeterminacy of rights in general. Rights claims, the argument goes, are mere definitional shells ready to be stuffed

---

[135] S. REP. NO. 105-190, at 18 (1998).

with their users' desires.[136] Even worse, because rights are formalistic rather than substantive, they are always vulnerable to redeployment by the most powerful actors in society, i.e., those with the resources to bend legal arguments and institutions in their favor.[137] Accordingly, competing claims on privacy in the DRM debates may simply camouflage other, more entrenched interests.

On its face, this explanation bodes poorly for contemporary efforts to conceptualize privacy in the digital age. Any definition—whether spatial, transactional, contextual, or other—can be twisted like a möbius strip to justify opposing ends. Pirates or other activists might choose to invoke privacy interests to gain temporary ground over copyright holders. But in the long-term, attempts to stabilize the meaning of information privacy will fall short.

In a second account, the DRM debates present no conundrum at all because the arguments on one side are far more credible than those on the other. After all, disagreement does not itself establish indeterminacy. Anti-DRM arguments might be far more convincing an application of privacy interests, for instance, and pro-DRM claims merely strategic rhetoric designed to confuse regulators. But regardless of which arguments appear more viable in hindsight, the actual proliferation of DRM tools, and the persistence of anti-circumvention laws, show that pro-DRM advocates have won in practice. If anti-DRM advocates had the better legal claims, then—once again—privacy arguments must not have been determinative at all.

A third account for the DRM debates turns to the technology itself; something about DRM tools might have caused the instability of the privacy claims about them. Perhaps the designs of some types of DRM technologies inherently favor certain privacy interests over others—say those of information producers rather than information

---

[136] *See, e.g.*, Mark Tushnet, *An Essay on Rights*, 62 TEX. L. REV. 1363 (1984) More recently, Jack Balkin has posited a theory of "ideological drift." Jack M. Balkin, *Ideological Drift and the Struggle Over Meaning*, 25 CONN. L. REV. 869, 871 (1993) ("Ideological drift in law means that legal ideas and symbols will change their political valence as they are used over and over again in new contexts."). Amy Kapczynski offers a way to conceive of simultaneous conflicting interpretations of rights and interests, rather than their evolution over time, when she contends that law exerts a gravitational pull to develop a "language of common disagreement between opposing groups." Amy Kapczynski, *The Access to Knowledge Mobilization and the New Politics of Intellectual Property*, 117 YALE L.J. 804, 810 (2008).

[137] *See, e.g.*, Morton J. Horwitz, *The Rule of Law: An Unqualified Human Good?*, 86 Yale L.J. 561, 566 (1977) ("By promoting procedural justice [law] enables the shrewd, the calculating, and the wealthy to manipulate its forms to their own advantage.").

consumers. The trick in this scenario would be how to distinguish the technologies that enhance certain goals from those that harm them. Once that evaluation has been made, struggles over the tool could take place completely independent from how legal institutions—or privacy law scholars—define privacy rights and interests.

Alternately, the umbrella category "DRM" may be such a general term, encompassing so many diverse tools, that any inherent structural biases in particular devices could wash out in the set as a whole. According to this account, pro-privacy claimants on conflicting sides of the DRM debates could share identical concepts and valuations of informational privacy but reference entirely different technologies. The real issue is which species of tools within the DRM-genus will shape law and policy.

The problem with these tool-based accounts, however, is that both sides of the debate make claims on each type of DRM device, including both access restrictions and tracking tools. Perhaps instead, then, individual DRM technologies are neutral as to competing privacy interests. A classic conception of technological neutrality would suggest that DRM could be dual-use, at once both a threat and protector to privacy. After all, DRM enables information control regardless of the content of that information. By extension, restrictions on the flow of information more generally may also be privacy-neutral. Pro-privacy claimants would thus reach opposite conclusions by focusing on different applications of the same tools.[138]

Yet, even seemingly neutral tools may be put to predominantly privacy-invasive uses. DRM might in theory apply equally to all categories of information. In practice, safeguarding one's interests using these tools could require resources and technological savvy more commonly available to institutional copyright holders than to individual consumers. In that case, copyright representatives will predictably argue in favor of the technology, and consumer advocates against it. Still, no innate quality of DRM would determine these arguments. In a world with different resource allocations the same tools would tend to serve other uses and inspire different claims. Hence, the core issue in this scenario is who uses the tool and for what ends.[139]

---

[138] Contrast this idea of technological neutrality with the critical work of Laura DeNardis, arguing that Internet technologies are a "control system" and a "proxy for state power." Laura DeNardis, *Internet Architecture as Proxy for State Power*, IP JUSTICE J. (Aug. 15, 2015) http://www.ipjustice.org/digital-rights/internet-architecture-redesign-as-proxy-for-state-power-by-laura-denardis/ [http://perma.cc/FDP4-K3V8].

[139] *See, e.g.*, Jack M. Balkin, *The Path of Robotics Law*, 6 CAL. L. REV. CIRCUIT 45, 59 (2015) (arguing "against essentialism in law's encounter with technology, advocating instead that we should always keep the social

It is plausible, then, that neither the characteristics of privacy nor of technology explain the issue; both might be red herrings that distract from other more powerful determinant interests key to understanding the DRM debates. Anti-DRM advocates and privacy law scholars both should thus focus their efforts away from theory towards the situated interests of technology users.[140]

V. Conclusion

Privacy-based anti-DRM arguments are part of a broader turn towards fundamental rights claims by those seeking intellectual property reforms. [141] Implementation of the Agreement on Trade-Related Aspects of Intellectual Property (TRIPS), for example, brought unprecedented scholarly attention to the human rights implications of intellectual property. Commenting on this phenomenon in 2006, Christophe Geiger argued that both utilitarian and natural law rationales for copyright failed on their own, but can be synthesized into an improved foundation of fundamental rights.[142] Others warned of a need to define the "attributes" of fundamental rights claims lest they be used to oppose intellectual property reform.[143] Considering the effectiveness of one instance of this larger pattern—pro-privacy anti-DRM claims—may offer insights into the operation of fundamental rights claims in intellectual property debates more broadly.

Despite the nuances to privacy implied by privacy law scholarship's conceptual struggle, advocates for legal reform of various kinds may eschew such fine conceptual parsing in favor of blanket invocations of privacy interests with potential for broader appeal. At the same time, the fact that contemporary pro-privacy social movements are politically heterogeneous may heighten the risk of redeployment. After the leak of classified information by Edward Snowden in 2013, for instance, advocacy organizations and corporations from across

---

aspects of technology in mind").

140 *See, e.g.*, Jack M. Balkin, *The Path of Robotics Law*, 6 CAL. L. REV. CIRCUIT 45, 59 (2015).

141 Paul Torremans, Daniel Gervais, Larry Helfer, Peter Yu, Catherine Ng, Dev Gangjee, Jonathan Griffiths, Peter Jaffey, and Tanya Aplin are among the many other scholars who have explored this arena. For an overview of the field circa 2008, see generally INTELLECTUAL PROPERTY AND HUMAN RIGHTS (Paul L.C. Torremans ed., 2008).

142 Christophe Geiger, *"Constitutionalising" Intellectual Property Law? The Influence of Fundamental Rights on Intellectual Property in the European Union*, 37 INT'L REV. OF INTELL. PROP. & COMPETITION L. 371, 382 (2006); *see also*, Peter K. Yu, *Ten Common Questions About Intellectual Property and Human Rights*, 23 GA. ST. U.L. REV. 709, 709 (2006).

143 Laurence R. Helfer, *Toward a Human Rights Framework for IP*, 40 U.C. DAVIS L. REV. 971, 976-77 (2006).

the political spectrum marched on Washington, D.C. to protest mass surveillance.[144] Left progressives from Demand Progress joined Public Citizen liberals to link hands with conservative libertarians from FreedomWorks and the Competitive Enterprise Institute.[145] In the words of one rally speaker, "This is an effort that is uniting strange bedfellows."[146]

Intellectual property reform advocates comprise similarly varied alliances: The "access to knowledge" movement has been described by Yochai Benkler as a "diverse coalition" of libertarians, liberals, leftists and anarchists.[147] Benkler credits the movement's success to human rights rhetorics that bridge "justice-seeking with freedom-seeking discourse."[148]

This Article suggests that short-term gains from "bridging" discursive strategies may carry long-term risks. Laurence Helfer has emphasized the need to define the "attributes" of fundamental rights claims lest they "bolster arguments . . . *against* revising intellectual property protection."[149] Or as Kapczynski observed in analyzing the formation of the access to knowledge movement, interpretive frames "generate opportunities for a group's opponents and make possible unpredictable chains of argument and counterargument."[150] Conceptual instability may raise the likelihood that invocations of privacy rights and interests will enhance early coalition building while laying groundwork for future conflict.

---

[144] STOP WATCHING US, https://rally.stopwatching.us (last visited June 1, 2015).

[145] *Id.*

[146] Stop Watching Us, *Rally Against Mass Surveillance 10/26/13*, YOUTUBE (Oct. 31, 2013), https://www.youtube.com/watch?t=75&v=BrtOZyGL3ww [https://perma.cc/7YNM-7LQY] ("I'm proud to stand here with democrats, with republicans, with progressives, with libertarians, because this is not about right and left. This is about right and wrong.").

[147] Yochai Benkler, *The Idea of Access to Knowledge: Long Term Trends and Basic Elements*, *in* ACCESS TO KNOWLEDGE IN THE AGE OF INTELLECTUAL PROPERTY 217, 230 (Gaëlle Krikorian & Amy Kapczynski eds., 2010).

[148] *Id.* at 235. Similarly, Peter Yu has identified "a growing need to develop a human rights framework for intellectual property." Peter K. Yu, *Reconceptualizing IP Interests in a Human Rights Framework*, 40 U.C. DAVIS L. REV. 1039, 1149 (2006).

[149] Laurence R. Helfer, *Toward a Human Rights Framework for IP*, 40 U.C. DAVIS L. REV. 971, 976-77 (2006).

[150] Kapczynski, *The Access to Knowledge Mobilization*, *supra* note 136, at 820.